TOLWORTH SCHOOL DATA PROTECTION POLICY & PROCEDURES

Governors' Committee Responsible Delegated to	Full Governing Body Headteacher and Data Protection Officer
Status	Statutory
Review Cycle	Annual
Date written	Sep 2021
Date of last review	Sep 2025
Date of next review	Sep 2026

Copyright © 2024 | [Tolworth School]

Contents

1 Policy Statement 4

2 Purpose 4

3 Scope 4

3.1 Definitions 5

4 Data Protection Background 6

4.1 National Data Protection Law 7

4.2 General Data Protection Regulation (GDPR) 7

4.2.1 Personal Data 7

4.2.2 The GDPR Principles 7

4.3 The Information Commissioners Office (ICO) 8

4.4 Data Protection Officer 9

4.4.1 Duties of the Data Protection Officer 9

5 Objectives 10

6 Governance Procedures 11

6.1 Accountability & Compliance 11

6.1.1 Privacy by Design 12

6.1.2 Information Audit 14

6.2 Legal Basis for Processing *(Lawfulness*) 14

6.2.1 Processing Special Category Data 15

6.2.2 Records of Processing Activities 16

6.3 Codes of Conduct & Certification Mechanisms 16

6.4 Third-Party Processors 17

6.5 Data Retention & Disposal 18

7 Data Protection Impact Assessments (DPIA) 19

8 Data Subject Rights Procedures 20

8.1 Consent & The Right to be Informed 20

8.1.1 Consent Controls 21

8.1.2 Alternatives to Consent 22

Copyright © 2024 | [Tolworth School]

8.1.3 Information Provisions....22
8.2 Privacy Policy & Notices....23
8.3 Personal Data Not Obtained from the Data Subject....25
8.3.1 Employee Personal Data....25
8.4 The Right of Access....25
8.4.1 Subject Access Request....26
8.5 Data Portability....27
8.6 Rectification & Erasure....27
8.6.1 Correcting Inaccurate or Incomplete Data....27
8.6.2 The Right to Erasure....28
8.7 The Right to Restrict Processing....28
8.8 Objections and Automated Decision Making....29
9 Oversight Procedures....30
9.1 Security & Breach Management....30
9.2 Passwords....30
10 Transfers & Data Sharing....31
11 Audits & Monitoring....31
12 Training....32
13 Penalties....32
14 Responsibilities....33

Copyright © 2024 | [Tolworth School]

1 POLICY STATEMENT

The Federation of Tolworth Infant, Nursery and Junior Schools (Tolworth School) needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from children, parents, employees, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)***, ***UK data protection laws*** and any other relevant the data protection laws and codes of conduct *(herein collectively referred to as **"the data protection laws"**).*

The School has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a ***'Privacy by Design'*** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2 PURPOSE

The purpose of this policy is to ensure that the School meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and in the individuals best interest.

The data protection laws include provisions that promote accountability and governance and as such the school has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

3 SCOPE

This policy applies to all staff within the School *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and*

Copyright © 2024 | [Tolworth School]

agents engaged with the School in the UK or overseas), and pertains to the processing of personal information. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.1 DEFINITIONS

- ***"Biometric data"*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- ***"Binding Corporate Rules"*** means personal data protection policies which are adhered to by the School for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
- ***"Consent"*** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- ***"Cross Border Processing"*** means processing of personal data which: -
    - takes place in more than one Member State; or
    - which substantially affects or is likely to affect data subjects in more than one Member State
- ***"Data controller"*** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- ***"Data processor"*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- ***"Data protection laws"*** means for the purposes of this document, the collective description of the GDPR, Data Protection Bill and any other relevant data protection laws that the School complies with.
- ***"Data subject"*** means an individual who is the subject of personal data
- ***"GDPR"*** means the *General Data Protection Regulation (EU) (2016/679)*
- ***"Genetic data"*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- ***"Personal data"*** means any information relating to an identified or identifiable natural person *('data subject'*); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Copyright © 2024 | [Tolworth School]

- ***"Processing"*** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- ***"Profiling"*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- ***"Recipient"*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- ***"Supervisory Authority"*** means an independent public authority which is established by a Member State
- ***"Third Party"*** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

4 DATA PROTECTION BACKGROUND

The UK initially had The Data Protection Act 1984 in place to regulate the use of processed information that related to individuals. However, in 1995 the introduction of EU Directive 95/46/EC which set aims and requirements for member states on the protection of personal data when processing or sharing, meant an updated Act was required.

The UK subsequently developed and enacted The Data Protection Act 1998 (DPA) to ensure that British law complied with the EU Directive and to provide those with obligations under the Act, with updated rules, requirements and guidelines for processing and sharing personal data.

2018 marks the 20th anniversary of the DPA enactment and whilst there have been periodical additions or alterations to the Act, technology has advanced at a far faster rate, necessitating new regulations for the current digital age. The past 20 years has also seen a vast increase in the number of businesses and services operating across borders, further highlighting the international inconsistency in Member States individual the data protection laws.

For this reason, in January 2012, the European Commission proposed a new regulation applying to all EU Member States and bringing a standardised and consistent approach to the processing and sharing of personal information across the EU.

Copyright © 2024 | [Tolworth School]

4.1 NATIONAL DATA PROTECTION LAW

As the School is in the UK, we are obligated under the GDPR and the UK's Data Protection Bill that implements the GDPR into UK law. Our data protection policies and procedures adhere to both the GDPR and Data Protection Bill requirements, as applicable to our business type.

4.2 GENERAL DATA PROTECTION REGULATION (GDPR)

The ***General Data Protection Regulation (GDPR) (EU)2016/679)*** was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to the Member States, replacing their existing local the data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the School processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the data protection laws and its principles.

4.2.1 PERSONAL DATA

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The School ensures that a high level or care and measures are afforded to personal data falling within the GDPR's **'special categories'** (previously **sensitive personal data**), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that: -

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies."

4.2.2 THE GDPR PRINCIPLES

Article 5 of the data protection laws requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes

Copyright © 2024 | [Tolworth School]

in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')*** and requires that firms ***show how*** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

4.3 THE INFORMATION COMMISSIONERS OFFICE (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Act 2018
- General Data Protection Regulation *(post-25th May 2018)*
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

The ICO's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and

Copyright © 2024 | [Tolworth School]

responding to complaints with regards to the data protection laws and those firms located solely in the UK.

4.4 DATA PROTECTION OFFICER

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by a firm where: -

- The processing is carried out by a public authority or body *(except for courts acting in their judicial capacity)*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

Where the School has appointed a designated DPO , we have done so in accordance with the GDPR requirements and have ensured that the assigned person has an adequate and expert knowledge of data protection law and practices and is fully able to, and capable of, assisting the School, as the controller/processor, in monitoring our internal compliance with the Regulation and to support and advise employees and associated third parties with regards to data protection laws and requirements.

4.4.1 DUTIES OF THE DATA PROTECTION OFFICER

The Data Protection Officer has assumed the below duties in compliance with GDPR Article 39: -

- To inform and advise the School and any employees carrying out processing, of their obligations pursuant to the GDPR, the Supervisory Authorities guidelines and any associated data protection provisions
- To monitor compliance with the GDPR, associated data protection provisions and the School's own data protection policies, procedures and objectives
- To oversee the assignment of responsibilities, awareness-raising and training of staff involved in processing operations
- To carry out and review audits of the above-mentioned policies, procedures, employee duties and training programs
- To cooperate with the Supervisory Authority where required
- To act as the point of contact for the Supervisory Authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter
- In accordance with Article 35 *(type of processing is likely to result in a high risk to the rights and freedoms of natural persons*), the DPO will provide advice where requested with regards to any data protection impact assessment and monitor its performance pursuant

Copyright © 2024 | [Tolworth School]

- Have due regard to, and be aware of, the risk associated with processing operations, considering the nature, scope, context and purposes of processing

Designated Data Protection Officer

NAME:	GDPR Sentry Limited
POSITION:	Data Protection Officer
ADDRESS:	Unit 434 Birch Park
	Thorp Arch Estate
	Wetherby
	West Yorkshire LS 23 7FG
EMAIL:	info@gdprsentry.com
TEL:	0113 804 2035

5 OBJECTIVES

We are committed to ensuring that all personal data processed by the School is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their data protection rights.

The School has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the regulatory requirements.

The School ensures that: -

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the School, is monitored for compliance with the data protection laws and its principles
- Data is only processed where we have met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR regulations and in compliance with the Data Protection Bill Schedule 1 requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees (*including new starters and agents*) are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their role and our business
- Individuals feel secure when providing us with personal information and know that it will be

Copyright © 2024 | [Tolworth School]

handled in accordance with their rights under the data protection laws

- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and GDPR news and updates, to stay abreast of updates, notifications and additional requirements
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed a Data Protection Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance
- We provide clear lines of reporting and supervision with regards to data protection
- We store and destroy all personal information, in accordance with the data protection laws timeframes and requirements
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13 & 14 information disclosures
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements
- We have developed and documented appropriate technical and organisational measures and controls for personal data security

6 GOVERNANCE PROCEDURES

6.1 ACCOUNTABILITY & COMPLIANCE

Due to the nature, scope, context and purposes of processing undertaken by the School, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have also implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws and any codes of conduct that we have obligations under.

We can demonstrate that all processing activities are performed in accordance with the data protection laws and that we have in place robust policies, procedures, measures and controls for the protection of data.

Copyright © 2024 | [Tolworth School]

Our main governance objectives are to: -

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all staff
- Identify key senior stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that the School has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated policies.

6.1.1 PRIVACY BY DESIGN

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We therefore have additional measures in place to adhere to this ethos, including: -

Data Minimisation

Under Article 5 of the data protection laws, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimal approach. We only ever obtain, retain, process and share the data that is essential to carry out our services and legal obligations and we only keep if for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection *(i.e. forms, website, surveys etc*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include 'optional' fields, as optional denotes that it is not necessary to obtain
- Physical collection *(i.e. face-to-face, telephone etc*) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- We have SLA's (Service Level Agreements) and bespoke agreements in place with third-party controllers who send us personal information (*either in our capacity as a controller or processor).* These state that only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.
- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement.

Copyright © 2024 | [Tolworth School]

Pseudonymisation

We utilise pseudonymisation where possible to record and store personal data in a way that ensures data can no longer be attributed to a specific data subject without the use of separate additional information (*personal identifiers*). Encryption and partitioning is also used to protect the personal identifiers, which are always kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation means that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption

Although we class encryption as a form of pseudonymisation, we also utilise it as a secondary risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Protection Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Restriction

Our *Privacy by Design* approach means that we use School-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the School's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by The Bursars, Headteacher and Deputy Headteachers.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (*i.e. copies of patient records, hospital invoices or claims information*). Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for. ***Steps include: -***

- In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject
- Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (*i.e. when the data is being passed to a third-party for processing and not directly to the data subject*)
- When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (*i.e. we do not use the postal system as this can be intercepted*). Where items are

Copyright © 2024 | [Tolworth School]

required in hard copy, we use the RBK secure courier service

- Recipients (*i.e. the data subject, third-party processer*) are reverified and their identity and contact details checked
- The Data Protection Officer authorises the transfer and checks the file(s) attached and encryption method and key
- Once confirmation has been obtained that the recipient has received the personal information, where possible *(within the legal guidelines and rules of the data protection laws*), we destroy the hard copy data and delete the sent message
- If for any reason a copy of the paper data must be retained by the School, we use a physical safe to store such documents as oppose to our standard archiving system

6.1.2 INFORMATION AUDIT

To enable the School to fully prepare for and comply with the data protection laws, we have carried out a School-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our School in our capacity as a controller/processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Disclosures and Transfers

6.2 LEGAL BASIS FOR PROCESSING *(LAWFULNESS)*

At the core of all personal information processing activities undertaken by the School, is the assurance and verification that we are complying with Article 6 of the data protection laws and our lawfulness of processing obligations. Prior to carrying out any processing activity on personal information, we always identify and establish the legal basis for doing so and verify these with the regulations.

This legal basis is documented on our information audit register and where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. ***Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -***

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or

Copyright © 2024 | [Tolworth School]

in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the School
- Processing is necessary for the purposes of the legitimate interests pursued by the School or by a third party (*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).*

6.2.1 PROCESSING SPECIAL CATEGORY DATA

Special categories of Personal Data are defined in the data protection laws as: -

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the School processes any personal information classed as special category data or information relating to criminal convictions, we do so in accordance with the data protection laws Article 9 regulations and in compliance with the Data Protection Bill's Schedule 1 Parts 1, 2, 3 & 4 requirements.

We will only ever process special category data where: -

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of

Copyright © 2024 | [Tolworth School]

health or social care or treatment or the management of health or social care systems and services

- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Schedule 1, Parts 1, 2 & 3 of The Data Protection Bill provide specific conditions and circumstances when special category personal data can be processed and dictated the requirements that organisations are obligated to meet when processing such data.

Where the School processes personal data that falls into one of the above categories, we have the specified provisions and measures in place prior to any processing. ***Measures include: -***

- Verifying our reliance on one of the data protection laws Article 9(1), and where applicable The Data Protection Bill Sch.1, Pt.1, Pt.2 and/or Pt.3 conditions prior to processing
- Having an appropriate policy document in place when the processing is carried out, specifying our: -
    - procedures for securing compliance with the data protection laws principles
    - policies as regards the retention and erasure of personal data processed in reliance on the condition
    - retention periods and reason *(i.e. legal, statutory etc)*
    - procedures for reviewing and updating our policies in this area

Please refer to our Retention & Erasure Policy for further guidance and procedures.

6.2.2 RECORDS OF PROCESSING ACTIVITIES

As an organisation with ***less than*** 250 employees, the School maintains records of all processing activities where: -

- Processing personal data could result in a risk to the rights and freedoms of individual
- The processing is not occasional
- We process special categories of data or criminal convictions and offences
- Such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Supervisory Authority upon request.

6.3 CODES OF CONDUCT & CERTIFICATION MECHANISMS

The School adheres to the data protection codes of conduct prepared by **the Senior Leadership Team and Bursar** and are certified by **the Governing Body** to demonstrate that we comply with the data protection laws rules and principles.

These codes and certification mechanism are approved by the Supervisory Authority and have been disseminated throughout the School to ensure competency and compliance from all staff.

Copyright © 2024 | [Tolworth School]

The codes of conduct that we adhere to help us to: -

- Improve transparency and accountability
- Demonstrate to the public and Supervisory Authority that we meet the requirements of the data protection law and that we can be trusted with personal data
- Mitigate against enforcement action(s)
- Improve standards by establishing best practice
- Carry out fair and transparent processing
- Ensure appropriate safeguards within the framework of personal data transfers to third countries or international organisations

We submit to frequent and unscheduled monitoring and audits by the codes of conduct association/trade body and by the data protection certification scheme and understand that where we are deemed to be non-compliant in any area relating to the data protection laws, we may lose our certification/seal of approval and/or the Supervisory Authority will be informed.

6.4 THIRD-PARTY PROCESSORS

The School utilise external processors for certain processing activities *(where applicable*). We use information audits to identify, categorise and record all personal data that is processed outside of the School, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. ***Such external processing includes*** *(but is not limited to****): -***

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources
- Credit Reference Agencies
- Direct Marketing Services

We have strict due diligence and Know Your Customer procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain School documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance. The continued protection of the rights of the data subjects is our priority when choosing a processor and we understand the importance of outsourcing processing activities as well as our continued obligations under the data protection laws even when a process is handled by a third-party.

We draft bespoke Service Level Agreements (SLAs) and contracts with each processor and among other details, outlines: -

- The processors data protection obligations

Copyright © 2024 | [Tolworth School]

- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

That contract or other legal act shall stipulate, in particular, that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the School in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to the School after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the School, all information necessary to demonstrate compliance with the obligations set out here and in the contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs the School immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

6.5 DATA RETENTION & DISPOSAL

The School have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and business requirements, as well as adhering to the data protection laws requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritises the protection of the personal data at all times.

Please refer to our ***Data Retention & Erasure Policy*** for full details on our retention, storage, periods and destruction processes.

Copyright © 2024 | [Tolworth School]

7 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the School. We therefore utilise several measures and tools to reduce risks and breaches for general processing, however when the processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where the School must, or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment*).

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced

Copyright © 2024 | [Tolworth School]

- Accepted

8 DATA SUBJECT RIGHTS PROCEDURES

8.1 CONSENT & THE RIGHT TO BE INFORMED

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by the School and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

The data protection law defines consent as; *'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.*

Where processing is based on consent, the School have reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand
- Pre-ticked, opt-in boxes are **never** used
- Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is **not** be a precondition of any service (*unless necessary for that service)*
- Along with our School name, we also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our School name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -

Copyright © 2024 | [Tolworth School]

- Opt-out links in mailings or electronic communications
- Opt-out process explanation and steps on website and in all written communications
- Ability to opt-out verbally, in writing or by email

- Consent withdrawal requests are processed immediately and without detriment
- Where services are offered to children, age-verification and parental-consent measures have been developed and are in place to obtain consent
- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified

8.1.1 CONSENT CONTROLS

The School maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent as it is to give consent.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Data Protection Officer prior to being circulated.

The data protection laws states that where processing is based on consent and the personal data relates to a child who is below the age of 16 years, such processing is only carried out by the School, where consent has been obtained by the holder of parental responsibility over the child. The UK's Data Protection Bill reduces this age to ***13 years***, as per Article 8(1) of the data protection laws what advises that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."*

Consent to obtain, process, store and share (*where applicable*), is obtained by the School through: -

- Face-to-Face
- Telephone
- In Writing
- Email/SMS
- Electronic *(i.e. via website form*)

Points 1-4 are enforced using scripts, checklists, on-screen prompts and signed customer agreements, to ensure that consent has been obtained and to remind employees of their additional consent obligations, as below.

Electronic consent is always by a non-ticked, opt-in action (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided. This is

Copyright © 2024 | [Tolworth School]

then followed up with an email, SMS or written confirmation of the consent to process, store and share the personal information.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

8.1.2 ALTERNATIVES TO CONSENT

The School recognise that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent, but would still process it even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use
- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate
- Where there is an imbalance in the relationship, i.e. with employees

8.1.3 INFORMATION PROVISIONS

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*)), we provide the below information in all instances, in the form of a consent/privacy notice: -

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party",* details of the legitimate interests
- The recipients or categories of recipients of the personal data *(if applicable)*
- If applicable, the fact that the School intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
    - where the School intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards the School has put into place and

Copyright © 2024 | [Tolworth School]

the means by which to obtain a copy of them or where they have been made available

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

8.2 PRIVACY POLICY & NOTICES

The terms Privacy Policy & Privacy Notice are used interchangeably when referring to data protection. This document is our ***Data Protection Policy*** and is an internal document designed to define the School's controls, procedures and objectives for securing, processing, handling and protecting personal information and complying with the data protection laws.

The School uses the terms Privacy Notice, which is separate a separate document from our Data Protection Policy and is provided to individuals at the time we collect their personal *data (or at the earliest possibility where that data is obtained indirectly)*. Our Privacy Notice includes the Article 13 & 14 (*section 8.1.3 of this policy*) requirements as set out in the data protection laws and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations. We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the customer facing policy that provides the legal information on how we handle, process and disclose personal information.

The notice is easily accessible, legible, jargon-free and is available in several formats, dependant on the method of data collection: -

- Via our website
- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials

Copyright © 2024 | [Tolworth School]

- Printed media, adverts and financial promotions

With lengthy content being provided in the privacy notice and with informed consent being based on its contents, we have tested, assessed and reviewed our privacy notice to ensure usability, effectiveness and understanding.

We follow the below ICO preferred steps for testing, reviewing and auditing our privacy notice(s) and opt-in consent formats prior to use and to record such assessments.

1. Privacy Notices are drafted by the Data Protection Officer using the data protection laws requirements and with Supervisory Authority guidance

2. We utilise a select customer base to test the Privacy Notice in its varying formats and provide a feedback form for completion, verifying the below points: -

a. How did you use the Privacy Notice *(e.g. website, agreement, orally)?*
b. Did you find the information in the Privacy Notice easy to read, understand and access?
c. Did you gain a full understanding of how we intend to use your data, who it will be shared with and what your rights are?
d. Did you feel confident in giving consent to use your personal data after reading the notice information?
e. Was there anything you did not understand?
f. Did you find any errors?
g. What, if anything, would you like to see changed about the Privacy Notice?

3. All feedback responses are saved with a copy of the used Privacy Notice and improvements are made and recorded where applicable

4. Re-testing is carried out on a new set of customers to ensure variety and independent assessment and verification

5. After a successful test, the acceptable Privacy Notice is rechecked against the data protection laws and Supervisory Authority regulations and guidelines to ensure it still complies and is adequate and effective

6. The final Privacy Notice(s) are then authorised by Senior Management/Director(s) before being rolled out

Where we rely on consent to obtain and process personal information, we ensure that it is: -

- Displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing

Copyright © 2024 | [Tolworth School]

8.3 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

Where the School obtains and/or processes personal data that has **not** been obtained directly from the data subject, the School ensures that the information noted in section 9.1.1 of this policy is provided to the data subject within 30 days of our obtaining the personal data *(except for advising if the personal data is a statutory or contractual requirement).*

In addition to the information provided to the data subject section of this policy, we also provide information about: -

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure. Where the School intends to further process any personal data for a purpose ***other*** than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in the relevant section of this policy, we reserve the right not to provide the data subject with the information if: -

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by Union or Member State law to which the School is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

8.3.1 EMPLOYEE PERSONAL DATA

As per the data protection laws guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights.

8.4 THE RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Copyright © 2024 | [Tolworth School]

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

8.4.1 SUBJECT ACCESS REQUEST

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the School from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the Data Protection Officer as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Please refer to our external ***Subject Access Request Procedures*** for the guidelines on how an SAR can

Copyright © 2024 | [Tolworth School]

be made and what steps we take to ensure that access is provided under the data protection laws.

8.5 DATA PORTABILITY

The School provides all personal information pertaining to the data subject to them on request and in a format, that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the data protection laws concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from the School to a designated controller, where technically feasible.

We utilise the below formats for the machine-readable data: -

- HTML

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

8.6 RECTIFICATION & ERASURE

8.6.1 CORRECTING INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d), all data held and processed by the School is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

Copyright © 2024 | [Tolworth School]

The Data Protection Officer are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.6.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be Forgotten'*, the School complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the School is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

8.7 THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where the School restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The School will apply restrictions to data processing in the following circumstances: -

- Where an individual contest the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (*where it was necessary for the performance of a public interest task or purpose of legitimate interests*), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

Copyright © 2024 | [Tolworth School]

The Data Protection Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.8 OBJECTIONS AND AUTOMATED DECISION MAKING

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. ***Individuals have the right to object to: -***

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling*)
- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where the School processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on *'grounds relating to their particular situation*'. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, the School will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention. We also assess new systems and technologies for this same component prior to implementation. The School understands that decisions absent of human interactions can be

Copyright © 2024 | [Tolworth School]

biased towards individuals and pursuant to Articles 9 and 22 of the data protection laws, we aim to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: -

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual

In limited circumstances, the School will use automated decision-making processes within the guidelines of the regulations. ***Such instances include: -***

- Where it is necessary for entering into or performance of a contract between us and the individual
- Where it is authorised by law *(e.g. fraud or tax evasion prevention)*
- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where the School uses, automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

9 OVERSIGHT PROCEDURES

9.1 SECURITY & BREACH MANAGEMENT

Alongside our *'Privacy be Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, the School has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

9.2 PASSWORDS

Passwords are a key part of the School protection strategy and are used throughout the School to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach. Whilst passwords are also directly related to Information Security and Access Control, the School recognises to strong, effective and robust password controls and measures are imperative to the protection and security of personal information.

Copyright © 2024 | [Tolworth School]

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third-parties who are responsible for one or more account, system or have access to any resource that requires a password.

Transfers & Data Sharing

The School takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within the UK and EU are deemed less of a risk than a third country or an international organisation, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods. We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Officer authorises all EU transfers and verifies the encryption and security methods and measures.

10 AUDITS & MONITORING

This policy and procedure document details the extensive controls, measures and methods used by the School to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance

Copyright © 2024 | [Tolworth School]

- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

11 TRAINING

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its Principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our Training & Development Procedures and Induction Policy detail how new and existing employees are trained, assessed and supported and include: -

- GDPR Workshops & Training Sessions
- Assessment Tests
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the data protection laws requirements and out own objectives and obligations around data protection.

12 PENALTIES

The School understands our obligations and responsibilities under the data protection laws and Supervisory Authority and comprehend the severity of any breaches under the Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we breach the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. ***We recognise that: -***

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Copyright © 2024 | [Tolworth School]

13 RESPONSIBILITIES

The School has appointed a Data Protection Officer whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection. The DPO will work in conjunction with the Compliance Officer, IT Manager and Training Officer to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.

Copyright © 2024 | [Tolworth School]